阿里云
访问控制

最佳实践

文档版本：20190213

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

1 RAM 企业上云安全实践

本文为您介绍当企业上云之后，通过 RAM 进行安全管控，帮助您实现简单管理账号、统一分配权限、集中管控资源，建立安全完善的资源控制体系。

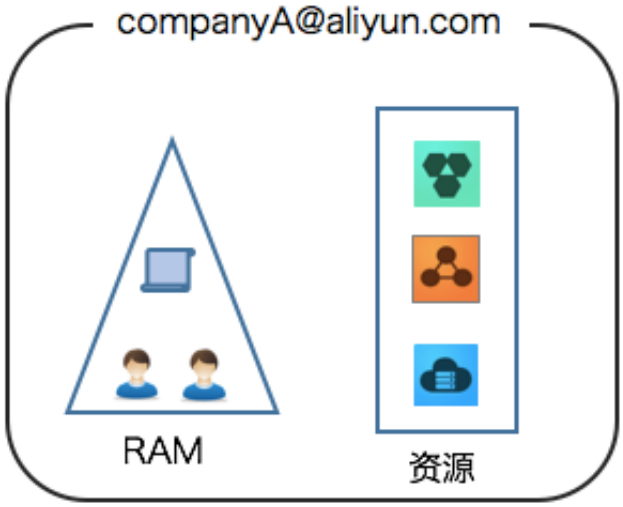
背景信息

某些公司使用 RAM 初期，对 RAM 的优势不够了解，也对云资源的安全管理要求不高，但是当初创企业成长为型公司，或大型企业客户迁移上云，他们的组织结构更加复杂，对云资源的安全管理需求也更加强烈。需要建立安全完善的资源控制体系。

- 存在多用户协同操作，RAM 用户分工不同，各司其职。
- 主账号不想与其他 RAM 用户共享主账号密钥，密钥泄露风险较大。
- RAM 用户对资源的访问方式多种多样，资源泄露风险高。
- 某些 RAM 用户离开组织时，需要收回其对资源的访问权限。

解决方案

使用 RAM，您可以创建、管理 RAM 用户，并可以控制这些 RAM 用户对资源的操作权限。当您的企业存在多用户协同操作资源时，使用 RAM 可以让您避免与其他用户共享主账号密钥，按需为用户分配最小权限，管理更加方便，权限更加明确，信息更加安全。



安全管理实施方案

- 创建独立的 RAM 用户

企业只需使用一个主账号。通过 RAM 为名下的不同操作员创建独立的 RAM 用户，进行分权管理，不使用主账号进行日常运维管理。

详情请参考：创建 *RAM* 用户。

- 将控制台用户与 API 用户分离

  不建议给一个 RAM 用户同时创建用于控制台操作的登录密码和用于 API 操作的访问密钥。

  - 对于应用程序账号，只需要通过 OpenAPI 访问云资源，只需要给它创建访问密钥即可。
  - 对于员工账号，只需要通过控制台操作云资源，只需要设置登录密码即可。

  详情请参考：创建 *RAM* 用户。

- 创建用户并进行分组

  当主账号下有多个 RAM 用户时，可以通过创建用户组对职责相同的 RAM 用户进行分类并授权。

  详情请参考：创建 *RAM* 用户组（可选）。

- 给不同用户组分配最小权限

  您可以使用系统策略为为用户或用户组绑定合理的权限策略，如果您需要更精细粒度的权限策略时，也可以选择使用自定义策略。通过为用户或用户组授予最小权限，可以更好的限制用户对资源的操作权限。

  详情请参考：权限策略管理。

- 为用户登录配置强密码策略

  您可以通过 RAM 控制台设置密码策略，如密码长度、密码中必须包含元素、密码有效期等。如果允许子用户更改登录密码，那么应该要求他们创建强密码并且定期轮换登录密码或访问密钥。

  详情请参考：*RAM* 初始设置。

- 给主账号开启多因素认证

  开启 MFA（Multi-factor authentication，多因素认证）可以提高账号的安全性，在用户名和密码之外再增加一层安全保护。启用 MFA 后，用户登录阿里云时，系统将要求输入两层安全要素：

  - 第一安全要素：用户名和密码。
  - 第二安全要素：来自其虚拟 MFA 设备的可变验证码。

  详情请参考：设置 MFA（可选）。

- 为用户开启SSO单点登录功能

开启SSO单点登录后，企业内部账号进行统一的身份认证，实现使用企业本地账号登录阿里云才能访问相应资源。

详情请参考：云账号的 *SAML* 配置。

- 不要为主账号创建访问密钥

  由于主账号对名下资源有完全控制权限，AccessKey 与登录密码具有同样的权力，AccessKey 用于程序访问，登录密码用于控制台登录。为了避免因访问密钥泄露带来的信息泄露，不建议您创建主账号访问密钥并使用该密钥进行日常工作。

  详情请参考：管理访问密钥。

- 使用策略限制条件来增强安全性

  要求用户必须使用安全信道（如 SSL）、在指定时间范围、或在指定源 IP 条件下才能操作指定的云资源。

  详情请参考：基本元素。

- 集中控制云资源

  阿里云默认主账号是资源的拥有者，掌握完全控制权。子账号对资源只有使用权，没有所有权。这一特性可以方便您对用户创建的实例或数据进行集中控制。

  - 当用户离开组织：只需要将对应的账号移除，即可撤销所有权限。
  - 当用户加入组织：只需创建新的账号，设置登录密码或访问密钥并为 RAM 用户授权。

  详情请参考：为 *RAM* 用户授权。

- 使用 STS 给临时用户授权

  STS （Security Token Service）是 RAM 的一个扩展授权服务，使用 STS 访问令牌可以给用户授予临时权限，您可以根据需要来定义访问令牌的权限和自动过期时间，可以让授权更加可控。

  详情请参考：*STS* 常见问题。

操作结果

遵循最佳安全实践原则，企业上云之后，综合利用这些保护机制，建立安全完善的资源控制体系，可以更有效的保护账号及资产的安全。

更多信息

企业上云以后通过 RAM 进行运维划分，根据指责不同，划分不同的运维人员，方便管理和控制。详情请参考：*RAM* 对多运维人员的权限管控。

2 RAM 对多运维人员的权限管控

当您的企业涉及多种运维需求时，通过 RAM 进行运维划分，对不同的运维人员授予不同的权限，方便管理和控制。

背景信息

某公司购买了大量的阿里云产品，并将应用系统部署在云上，因此涉及多种运维需求：

- 不同的运维负责人需要运维不同的阿里云产品。
- 不同的运维人员需要不同的访问、操作、管理云资源的权限。

运维划分解决方案

根据云产品进行运维划分，设置如下运维负责人并授予特定的权限策略。

图 2-1: 运维负责人

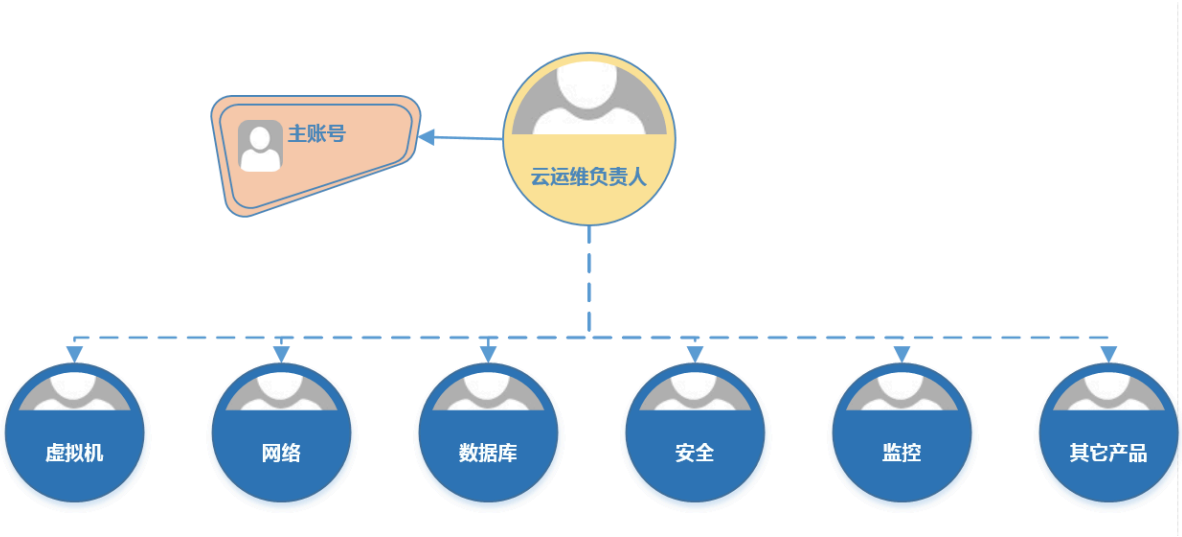


表 2-1: 权限策略

运维负责人	权限策略名称	权限策略说明
云运维负责人	AdministratorAccess	管理所有阿里云资源的权限
虚拟机运维负责人	AliyunECSFullAccess	管理云服务器服务（ECS）的权限
	AliyunESSFullAccess	管理弹性伸缩服务（ESS）的权限
	AliyunSLBFullAccess	管理负载均衡服务（SLB）的权限
	AliyunNASFullAccess	管理文件存储服务（NAS）的权限
	AliyunOSSFullAccess	管理对象存储服务（OSS）权限

运维负责人	权限策略名称	权限策略说明
	AliyunOTSFullAccess	管理表格存储服务（OTS）的权限
网络运维负责人	AliyunCDNFullAccess	管理CDN的权限
	AliyunCENFullAccess	管理云企业网（CEN）的权限
	AliyunCommonBandwidthPackageFullAccess	管理共享带宽的权限
	AliyunEIPFullAccess	管理弹性公网IP（EIP）的权限
	AliyunExpressConnectFullAccess	管理高速通道（ExpressConnect）的权限
	AliyunNATGatewayFullAccess	管理NAT网关（NATGateway）的权限
	AliyunSCDNFullAccess	管理安全加速（SCDN）的权限
	AliyunSmartAccessGatewayFullAccess	管理智能接入网关（SmartAccessGateway）的权限
	AliyunVPCFullAccess	管理专有网络（VPC）的权限
	AliyunVPNGatewayFullAccess	管理VPN网关（VPNGateway）的权限
数据库运维负责人	AliyunRDSFullAccess	管理云数据库服务（RDS）的权限
	AliyunDTSFullAccess	管理数据传输服务（DTS）的权限
安全运维负责人	AliyunYundunFullAccess	管理云盾所有产品（Yundun）的权限
监控运维负责人	AliyunActionTrailFullAccess	管理操作审计（ActionTrail）的权限
	AliyunARMSFullAccess	管理业务实时监控服务（ARMS）的权限
	AliyunCloudMonitorFullAccess	管理云监控（CloudMonitor）的权限
	ReadOnlyAccess（可选）	只读访问所有阿里云资源的权限（可选）
	AliyunSupportFullAccess	管理工单系统的权限

示例：将用户配置为数据库运维负责人

此示例将 RAM 用户`alice@secloud.onaliyun.com`配置为数据库运维负责人，从而允许该用户管理云数据库服务（RDS）和数据传输服务（DTS）。

1. 登录 *RAM* 控制台。

2. 创建 *RAM* 用户为`alice@secloud.onaliyun.com`。
3. 找到创建好的 RAM 用户，单击添加权限 。
4. 从左侧权限策略名称列中勾选`AliyunRDSFullAccess`和`AliyunDTSFullAccess`，单击确定。

> **说明:**
> 如需将用户配置为其他运维负责人，请参考上述权限策略表格，为相关负责人授予相应的权限。

更多信息

如需了解详细运维案例，请参考 阿里云*RAM*运维最佳实践。

3 利用标签对 ECS 实例进行分组授权

本文介绍了如何利用标签对 ECS 实例进行分组并授权，以满足 RAM 用户只能查看和操作被授权资源的需求。

背景信息

假设您的账号购买了 10 个 ECS 实例，其中 5 个想要授权给 dev 团队，另外 5 个授权给 ops 团队。企业希望每个团队只能查看被授权的实例，未被授权的不允许查看。

分组授权的前提条件

请确保已拥有 RAM 账号并可以登录 *RAM* 控制台。

分组授权解决方案

创建两个用户组，通过打标签将 ECS 实例分成 2 个组并授权给对应的用户组。

- 其中 5 个实例打上一对标签，标签键是 team，标签值是 dev。
- 另外 5 个实例打上另一对标签，标签键是 team，标签值是 ops。

分组授权的操作步骤

1. 登录 ECS 控制台，选择一个实例，在操作菜单下选择更多 > 实例设置 > 编辑标签。
2. 单击新建标签，输入标签键和标签值，单击确定。

   说明:
   将所有机器分别打上对应的标签。
3. 登录 RAM 控制台创建两个用户组： dev 和 ops。

   详情请参考：创建 *RAM* 用户组（可选）。
4. 创建不同的 RAM 账号，并添加到相应的用户组下。

   详情请参考：创建 *RAM* 用户。
5. 创建两个自定义策略，分别授权给两个用户组。

   详情请参考：*RAM* 授权。

   说明:
   授权后 RAM 用户已继承对应用户组的相关权限。

   例如：给 dev 组授权的自定义策略名称是 policyForDevTeam，策略内容如下：

```
{
```

```
    "Statement": [
    {
        "Action": "ecs:*",
        "Effect": "Allow",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "ecs:tag/team": "dev"
            }
        }
    },
    {
        "Action": "ecs:DescribeTag*",
        "Effect": "Allow",
        "Resource": "*"
    }
    ],
    "Version": "1"
}
```

在上述权限策略中：

- 带有 Condition 的`"Action": "ecs:*"`部分用于过滤标签为`"team": "dev"`的资源。
- `"Action": "ecs:DescribeTag*"`用于展示所有标签。当 RAM 用户在操作 ECS 控制台时，系统展示出所有标签供 RAM 用户选择，只有当 RAM 用户选择了标签值后，系统才能根据选中的标签值过滤相应资源。

> 说明：
> 根据上述自定义策略，创建另一个 policyForOpsTeam 权限策略并授权给 ops 用户组。

显示被授权实例

1. RAM 用户登录 ECS 控制台。

   > 说明：
   > 登录控制台后，系统默认跳转到 ECS 概览页，此时 RAM 用户看到的实例数为 0，如需查看相关实例，请切换到实例页签下。

2. 单击实例，单击搜索栏旁的标签。

   > 说明：
   > 请确保控制台展示的当前地域是期望地域。

3. 鼠标悬停在标签键上，在标签键下拉列表的右侧会展示出对应的标签值，点击对应的标签值，系统可以过滤出相应资源。

   > 说明：
   > 选中标签值之后，系统才可以过滤出相应资源。

更多信息

利用标签对安全组、云盘、快照、镜像进行分组授权的方法与上述对实例分组授权的方法相同。

说明:

镜像中只有自定义镜像支持打标签。

4 利用标签对 RDS 实例进行分组授权

本文介绍了如何利用标签对 RDS 实例进行分组并授权，以满足 RAM 用户只能查看和操作被授权资源的需求。

背景信息

假设您的账号购买了 10 个 RDS 实例，其中 5 个想要授权给 dev 团队，另外 5 个授权给 ops 团队。企业希望每个团队只能查看被授权的实例，未被授权的不允许查看。

利用标签对 RDS 分组授权的操作步骤

具体操作步骤请参考利用标签对 *ECS* 实例进行分组授权。

RDS 相关自定义策略：

```
{
  "Statement": [
    {
      "Action": "rds:*",
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "rds:ResourceTag/team": "dev"
        }
      }
    },
    {
       "Action": "rds:DescribeTag*",
       "Effect": "Allow",
       "Resource": "*"
     }
  ],
  "Version": "1"
}
```

权限策略内容分为两部分：

- 其中带有 Condition 的`"Action": "rds:*"`部分用于过滤标签为`"team": "dev"`的资源。Condition部分的关键字为`rds:ResourceTag`。
- `"Action": "rds:DescribeTag*"`用于展示所有标签。当 RAM 用户在操作 RDS 控制台时，系统展示出所有标签供 RAM 用户选择，只有当 RAM 用户选择了标签值后，系统才能根据选中的标签值过滤相应资源。

更多信息

利用标签对 RDS 实例分组授权后，如果遇到 RAM 用户登录控制台报无权限的问题，请参考：利用标签对 *RDS* 实例分组授权的常见问题。

5 使用 ActionTrail 记录 RAM 操作

ActionTrail 可以记录主账号或 RAM 用户进行的操作，通过 ActionTrail 可以查看所有用户对资源实例进行操作的记录。

前提条件

RAM 已经与 ActionTrail 服务进行了集成，可以联合使用。

使用 ActionTrail 查看 RAM 操作记录的步骤

1. 登录 *ActionTrail* 控制台。
2. 在历史事件查询页签下，使用过滤器进行搜索。
3. 输入相关的用户名，选择事件类型和时间后，单击搜索。

> **说明:**
> 您也可以通过事件名称、资源类型、资源名称、AccessKeyId等进行搜索。

4. 单击需要查看的事件，单击查看事件。

ActionTrail 记录的操作

ActionTrail 可以记录 RAM 的如下操作信息：

- 主账号或 RAM 用户的登录信息，详情请参考 *ConsoleSignin*。
- RAM 控制台的操作，例如：

```
{
    "apiVersion":"2015-05-01",
    "eventId":"2cc52dee-d8d2-40c2-8de0-3a2cf1df07a0",
    "eventName":"DeleteGroup",
    "eventSource":"ram.aliyuncs.com",
    "eventTime":"2015-11-03T13:41:49Z",
    "eventType":"ApiCall",
    "eventVersion":"1",
    "requestId":"9AE24F49-C52C-4F0F-BCF9-9A4B8C22B147",
    "requestParameters":{
        "GroupName":"grp1",
    },
    "serviceName":"Ram",
    "sourceIpAddress":"42.120.74.90",
    "userAgent":"AliyunConsole",
    "userIdentity":{
        "type":"ram-user",
        "principalId":"274180646548292385",
        "accountId":"43274",
        "userName":"Alice",
        "sessionContext":{
            "sessionAttributes":{
```

```
                "creationDate":"2015-11-03T13:41:48Z",
                "mfaAuthenticated":"true"
            }
        }
    }
}
```

- **RAM/STS 的所有创建、变更、删除类 API 调用信息，例如：**

```
{
    "apiVersion": "2015-05-01",
    "eventId": "234ef3c7-8938-4bd7-bb80-11754b7bdd4c",
    "eventName": "CreateGroup",
    "eventSource": "ram.aliyuncs.com",
    "eventTime": "2016-01-04T08:58:50Z",
    "eventType": "ApiCall",
    "eventVersion": "1",
    "recipientAccountId": "43274",
    "requestId": "1485748C-DB62-4693-AB7E-4BA3F3A970E1",
    "requestParameters": {
        "Comments": "this is a test group",
        "GroupName": "grp1"
    },
    "serviceName": "Ram",
    "sourceIpAddress": "42.120.74.96",
    "userAgent": "aliyuncli/2.0.6",
    "userIdentity": {
        "type": "ram-user",
        "principalId": "274180646548292385",
        "accountId": "43274",
        "accessKeyId": "f6IzzFZMmzNwEI4d",
        "userName": "Alice"
    }
}
```

更多信息

关于操作记录的详细信息，请参考操作事件(Event)结构定义。

6 云服务器 ECS 授权

问题

- 查看 ECS 的权限定义
- 为一个子用户授予 ECS 服务的完全管理权限
- 为一个子用户授予只读访问 ECS 的权限
- 仅允许子用户查看青岛的 ECS 实例，但是不允许查看磁盘信息及快照信息
- 授权一个子用户管理两台指定的 ECS 实例
- 授权子用户创建快照权限

查看 ECS 的权限定义

请参考 ECS OpenAPI 文档中的鉴权规则。

为一个子用户授予 ECS 服务的完全管理权限

在 RAM 控制台上，为此子用户（或该用户所在群组）附加系统授权策略 “AliyunECSFullAccess”。

为一个子用户授予只读访问 ECS 的权限

在 RAM 控制台中创建一个子用户，并为此子用户附加系统授权策略 “AliyunECSReadOnlyAccess”。

添加授权策略的方式请参考授权。

仅允许子用户查看青岛的 ECS 实例，但是不允许查看磁盘信息及快照信息

查看 ECS 资源列表的授权粒度可以到 “Region + 资源类型” 的级别。

下面的样例仅授权查看青岛的 ECS 实例信息。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ecs:DescribeRegions",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ecs:Describe*",
      "Resource": "acs:ecs:cn-qingdao:*:instance/*"
    }
  ],
  "Version": "1"
```

```
}
```

授权一个子用户管理两台指定的 ECS 实例

假设您的租户账号购买了 10 个 ECS 实例。而作为 RAM 管理员，您希望仅仅授权其中的 2 个 ECS 实例给某个 RAM 用户。那么您可以创建如下的自定义授权策略：

说明：

授予该策略的 RAM 用户是可以列出所有的 ECS 实例，但只能操作（比如 StopInstance 操作）其中的两台。目前，不支持 RAM 用户仅仅查看自己有访问权限的 ECS 实例。

这里假设您的两台实例 ID 分别是 i-001 和 i-002；首先您需要创建一条自定义授权策略，包含管理 i-001,i-002 的权限以及查看 ECS 所有资源的权限：

```
{
  "Statement": [
    {
      "Action": "ecs:*",
      "Effect": "Allow",
      "Resource": [
                  "acs:ecs:*:*:instance/i-001",
                  "acs:ecs:*:*:instance/i-002"
                  ]
    },
    {
      "Action": "ecs:Describe*",
      "Effect": "Allow",
      "Resource": "*"
    }
  ],
  "Version": "1"
}
```

然后为子用户附加该自定义授权策略即可。

授权子用户创建快照权限

如果已经授权给子账户指定 ECS 的管理员权限后，依然不能创建磁盘快照，因为快照是基于磁盘基础上，需要授予子用户指定磁盘的权限。

假设您需要指定子账户管理实例 ID 为 inst-01 的 ecs，并且具备给 ID 为：dist-01 的磁盘创建快照的权限。您可以创建如下的自定义授权策略：

```
{
  "Statement": [
    {
      "Action": "ecs:*",
      "Effect": "Allow",
      "Resource": [
        "acs:ecs:*:*:instance/inst-01"
      ]
    },
    {
      "Action": "ecs:CreateSnapshot",
```

```
      "Effect": "Allow",
      "Resource": [
        "acs:ecs:*:*:disk/dist-01",
        "acs:ecs:*:*:snapshot/*"
      ]
    },
    {
      "Action": [
        "ecs:Describe*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ],
  "Version": "1"
}
```

然后为子用户附加该自定义授权策略即可。

7 ECS授权样例

如果您的租户账号购买了10个ECS实例。而作为RAM管理员，您希望仅仅授权其中的2个ECS实例给某个RAM用户。那么您可以创建如下的授权策略：

说明：

授予该策略的RAM用户是可以列出所有的ECS实例，但只能操作（比如StopInstance操作）其中的两台。目前，不支持RAM用户仅仅查看自己有访问权限的ECS实例。

```
{
  "Statement": [
    {
      "Action": "ecs:*",
      "Effect": "Allow",
      "Resource": [
                  "acs:ecs:*:*:instance/i-001",
                  "acs:ecs:*:*:instance/i-002"
                  ]
    },
    {
      "Action": "ecs:Describe*",
      "Effect": "Allow",
      "Resource": "*"
    }
  ],
  "Version": "1"
}
```

8 对象存储 OSS 授权

问题

- 查看 OSS 的权限定义
- 为一个子用户授予只读访问 OSS 的权限
- 为一个子用户授予完全管理 OSS 的权限
- 授权一个子用户列出并读取一个 Bucket 中的资源
- 在OSS中使用带IP限制的访问控制
- OSS目录级别的授权
- 授权子用户完全管理某个 Bucket 的权限
- 子用户已经被授予了某Bucket权限，为什么登录OSS控制台访问时提示没有操作权限

查看 OSS 的权限定义

请参考 OSS 产品文档中的访问控制部分。

为一个子用户授予只读访问 OSS 的权限

在 RAM 控制台中创建一个子用户，并为此子用户附加系统授权策略”AliyunOSSReadOnlyAccess”。附加授权策略的方式请参考授权。

为一个子用户授予完全管理 OSS 的权限

在 RAM 控制台中为此子用户附加系统授权策略 “AliyunOSSFullAccess”。

授权一个子用户列出并读取一个 Bucket 中的资源

如果您需要授权一个子用户（例如，代表您的某个应用程序）通过 OSS SDK 或 OSS CMD 列出并读取一个 Bucket 中的资源，那么您需要创建一条自定义授权策略来完成。

假设您的 Bucket 名称为 “myphotos”，那么创建的授权策略样例如下：

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "oss:ListObjects",
            "Resource": "acs:oss:*:*:myphotos"
        },
        {
            "Effect": "Allow",
            "Action": "oss:GetObject",
            "Resource": "acs:oss:*:*:myphotos/*"
        }
    ]
```

```
}
```

如果您希望被授权的子用户能够通过 OSS 控制台进行操作，那么授权策略中还需要添加 GetBucketAcl 以及 GetObjectAcl 权限（控制台为了操作体验的优化需要额外调用 OSS 的部分 API）。允许子用户通过 OSS 控制台操作的授权策略样例如下：

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "oss:ListBuckets",
            "Resource": "acs:oss:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "oss:ListObjects",
                "oss:GetBucketAcl"
            ],
            "Resource": "acs:oss:*:*:myphotos"
        },
        {
            "Effect": "Allow",
            "Action": [
                "oss:GetObject",
                "oss:GetObjectAcl"
            ],
            "Resource": "acs:oss:*:*:myphotos/*"
        }
    ]
}
```

在OSS中使用带IP限制的访问控制

示例1: 在`Allow`授权中增加IP限制

允许通过`42.120.88.0/24`, `42.120.66.0/24`两个IP段读取myphotos中的信息;

```
{
    "Version": "1",
    "Statement": [
        {
            "Sid": "允许列出所有Bucket",
            "Effect": "Allow",
            "Action": [
                "oss:ListBuckets"
            ],
            "Resource": [
                "acs:oss:*:*:*"
            ]
        },
        {
            "Sid": "允许获取myphotos中的信息，访问源必须在允许的IP段中",
            "Effect": "Allow",
            "Action": [
                "oss:ListObjects",
                "oss:GetObject"
            ],
```

```
            "Resource": [
                "acs:oss:*:*:myphotos",
                "acs:oss:*:*:myphotos/*"
            ],
            "Condition":{
                "IpAddress": {
                    "acs:SourceIp": ["42.120.88.0/24", "42.120.66.0/24
"]
                }
            }
        }
    ]
}
```

示例2: 在Deny授权中增加IP限制

如果源IP不在42.120.88.0/24中，则禁止对OSS执行任何操作；

```
{
    "Version": "1",
    "Statement": [
        {
            "Sid": "允许列出所有Bucket",
            "Effect": "Allow",
            "Action": [
                "oss:ListBuckets"
            ],
            "Resource": [
                "acs:oss:*:*:*"
            ]
        },
        {
            "Sid": "允许获取myphotos中的信息",
            "Effect": "Allow",
            "Action": [
                "oss:ListObjects",
                "oss:GetObject"
            ],
            "Resource": [
                "acs:oss:*:*:myphotos",
                "acs:oss:*:*:myphotos/*"
            ]
        },
        {
            "Sid": "禁止从42.120.88.0/24以外访问OSS",
            "Effect": "Deny",
            "Action": "oss:*",
            "Resource": [
                "acs:oss:*:*:*"
            ],
            "Condition":{
                "NotIpAddress": {
                    "acs:SourceIp": ["42.120.88.0/24"]
                }
            }
        }
    ]
```

```
}
```

注意：因为Policy的鉴权规则是Deny优先(即如果用户的访问操作命中任意一条Deny规则，则禁止访问)，所以访问者从42.120.88.0/24以外的IP地址访问myphotos中的内容时，OSS服务会报没有权限。

OSS目录级别的授权

目录级别的授权属于授权的高级功能，如果您有此类需求，请您认真阅读并理解此部分。

背景

假设有一个用于存放照片的Bucket，叫myphotos。这个bucket下有一些目录，代表照片的拍摄地；每个拍摄地目录下又有年份子目录。

目录树结构如下

```
myphotos[Bucket]
   ├── beijing
   │   ├── 2014
   │   └── 2015
   ├── hangzhou
   │   ├── 2013
   │   ├── 2014
   │   └── 2015 //授予此目录只读权限
   └── qingdao
       ├── 2014
       └── 2015
```

假设我们需要授权一个子用户只读访问`myphotos/hangzhou/2015/`目录的只读权限。根据使用场景不同，授权策略也有很大的区别。下面我们根据授权策略的复杂程度，由简入繁的为大家介绍三种场景。

场景一：子用户知道所在文件的路径，只需要读取文件内容的权限，不需要列出文件的权限

这个场景的特点是子用户知道文件的完整路径，可以使用完整的文件路径直接去读取文件内容。通常我们会将这样的权限授予一个软件系统，系统中文件路径符合某种规则(比如文件名是员工工号)，或者文件路径持久化在软件系统的数据库中。

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "oss:GetObject"
            ],
            "Resource": [
                "acs:oss:*:*:myphotos/hangzhou/2015/*"
            ]
        }
    ]
```

```
}
```

场景二：子用户使用OSS CMD访问目录`myphotos/hangzhou/2015/`，但是不知道目录中有哪些文件，需要列出目录中文件的权限

通常会将这样的权限授予软件开发者。开发者不清楚目录中究竟有哪些文件，然后使用OSS CMD或API直接获取目录信息。

与场景一相比，这里需要新增ListObjects的权限。因为我们仅允许列出`myphotos/hangzhou/2015/`目录中的文件，所以在新增的ListObjects权限中，增加”oss:Prefix”的条件限定。

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "oss:GetObject"
            ],
            "Resource": [
                "acs:oss:*:*:myphotos/hangzhou/2015/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "oss:ListObjects"
            ],
            "Resource": [
                "acs:oss:*:*:myphotos"
            ],
            "Condition":{
                "StringLike":{
                    "oss:Prefix":"hangzhou/2015/*"
                }
            }
        }
    ]
}
```

场景三：子用户使用OSS控制台访问目录`myphotos/hangzhou/2015/`

最易用的场景，当子用户使用可视化的OSS客户端访问目录`myphotos/hangzhou/2015/`，可视化的客户端像Windows文件管理器一样，让子用户可以从根目录开始，一层一层的进入所要访问的目录。

与场景二相比，使用OSS可视化客户端时需要从从根目录一层一层导航进入`myphotos/hangzhou/2015/`，所以需要新增以下权限：

1. **列出所有Bucket的权限**
2. **列出myphotos下目录的权限，在这个例子中，即可以看到beijing/hangzhou/qingdao三个目录**

3. 列出myphotos/hangzhou下的目录的权限，即可以看到2013/2014/2015三个目录

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "oss:ListBuckets",
                "oss:GetBucketAcl"
            ],
            "Resource": [
                "acs:oss:*:*:*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "oss:GetObject",
                "oss:GetObjectAcl"
            ],
            "Resource": [
                "acs:oss:*:*:myphotos/hangzhou/2015/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "oss:ListObjects"
            ],
            "Resource": [
                "acs:oss:*:*:myphotos"
            ],
            "Condition": {
                "StringLike": {
                    "oss:Delimiter": "/",
                    "oss:Prefix": [
                        "",
                        "hangzhou/",
                        "hangzhou/2015/*"
                    ]
                }
            }
        }
    ]
}
```

授权子用户完全管理某个 Bucket 的权限

首先，创建一条自定义授权策略。假设您的 Bucket 名称为 “myphotos”。

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "oss:*",
            "Resource": [
                "acs:oss:*:*:myphotos",
                "acs:oss:*:*:myphotos/*"
            ]
        }
```

```
    ]
}
```

然后，为此用户添加此条自定义授权策略。

子用户已经被授权了某Bucket权限，为什么登录OSS控制台访问时提示没有操作权限

假设您已经授权某个子用户对某个Bucket（比如myphotos）拥有读取数据对象的操作权限：

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "oss:ListObjects"
      ],
      "Resource": "acs:oss:*:*:myphotos"
    },
    {
      "Effect": "Allow",
      "Action": [
        "oss:GetObject"
      ],
      "Resource": "acs:oss:*:*:myphotos/*"
    }
  ]
}
```

但是子用户登录OSS控制台仍然报错“没有相应操作权限”，这是为何呢?

因为当用户登录OSS控制台时，OSS控制台为以当前登录用户的授权身份去访问OSS服务。为了获得更好的交互体验，OSS控制台会额外调用ListBuckets操作，以及GetBucketAcl和GetObjectAcl操作（因为要确定bucket属性是公开或私有）。

所以，为了支持通过OSS控制台操作某个Bucket，相应的授权Policy如下所示：

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "oss:ListBuckets",
      "Resource": "acs:oss:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "oss:ListObjects",
        "oss:GetBucketAcl"
      ],
      "Resource": "acs:oss:*:*:myphotos"
    },
    {
      "Effect": "Allow",
      "Action": [
        "oss:GetObject",
        "oss:GetObjectAcl"
      ],
```

```
      "Resource": "acs:oss:*:*:myphotos/*"
    }
  ]
}
```

9 OSS授权样例

- Use Case #1

  如下的授权策略允许一个RAM用户通过OSS Web控制台对某个指定的OSS存储Bucket（比如myphotos）进行READ操作。

```
{
    "Version": "1",
    "Statement": [
    {
        "Effect": "Allow",
        "Action": "oss:ListBuckets",
        "Resource": "acs:oss:*:*:*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "oss:ListObjects",
            "oss:GetBucketAcl"
        ],
        "Resource": "acs:oss:*:*:myphotos"
    },
    {
        "Effect": "Allow",
        "Action": [
            "oss:GetObject",
            "oss:GetObjectAcl"
        ],
        "Resource": "acs:oss:*:*:myphotos/*"
    }
  ]
}
```

- Use Case #2

  如下的授权策略允许一个RAM用户通过OSS SDK对某个指定的OSS存储Bucket（比如myphotos）进行READ操作，但要求的限制条件为：请求者的SourceIP必须来自于”42.120.88.18”或“42.120.66.0/24”。

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "oss:ListBuckets"
            ],
            "Resource": [
                "acs:oss:*:*:*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "oss:ListObjects",
```

```
                "oss:GetObject"
            ],
            "Resource": [
                "acs:oss:*:*:myphotos",
                "acs:oss:*:*:myphotos/*"
            ],
            "Condition":{
                "IpAddress": {
                    "acs:SourceIp": ["42.120.88.18", "42.120.66.0/24
"]
                }
            }
        }
    ]
}
```

- **Use Case #3**

  如下的授权策略允许一个RAM用户通过OSS Web控制台对某个指定的OSS存储路径下的所有对象（比如myphotos/hangzhou/2015/）进行READ操作。

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "oss:ListBuckets",
                "oss:GetBucketAcl"
            ],
            "Resource": [
                "acs:oss:*:*:*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "oss:GetObject",
                "oss:GetObjectAcl"
            ],
            "Resource": [
                "acs:oss:*:*:myphotos/hangzhou/2015/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "oss:ListObjects"
            ],
            "Resource": [
                "acs:oss:*:*:myphotos"
            ],
            "Condition": {
                "StringLike": {
                    "oss:Delimiter": "/",
                    "oss:Prefix": [
                        "",
                        "hangzhou/",
                        "hangzhou/2015/*"
                    ]
                }
            }
```

```
            }
        ]
}
```

10 云数据库 RDS 授权

问题

- 查看 *RDS* 的权限定义
- 为一个子用户授予只读访问 *RDS* 的权限
- 为一个子用户授予 *RDS* 服务的完全管理权限
- 授权一个子用户管理两台指定的 *RDS* 实例
- 子用户访问 *DMS* 管理数据库内容

查看 RDS 的权限定义

请参考RDS资源授权。

为一个子用户授予只读访问 RDS 的权限

在 RAM 控制台中创建一个子用户，并为此子用户附加系统授权策略”AliyunRDSReadOnlyAccess”。添加授权策略的方式请参考授权。

为一个子用户授予 RDS 服务的完全管理权限

在 RAM 控制台中为此子用户附加系统授权策略 “AliyunRDSFullAccess”。

授权一个子用户管理两台指定的 RDS 实例

您需要使用自定义授权策略的功能。这里例如您的两台实例 ID 分别是 i-001 和 i-002。

首先您需要创建一条自定义授权策略，包含管理 i-001、i-002 的权限以及查看 RDS 所有资源的权限：

```
{
  "Statement": [
    {
      "Action": "rds:*",
      "Effect": "Allow",
      "Resource": [
                  "acs:rds:*:*:dbinstance/i-001",
                  "acs:rds:*:*:dbinstance/i-002"
                  ]
    },
    {
      "Action": "rds:Describe*",
      "Effect": "Allow",
      "Resource": "*"
    }
  ],
  "Version": "1"
```

```
}
```

然后为此用户添加此条自定义授权策略。

子用户访问 DMS 管理数据库内容

使用 DMS 访问 RDS 云数据库，对应的授权 Action 是 “dms:LoginDatabase”。

授权子用户登录指定 RDS

授权策略样例如下：

```
{
  "Statement": [
    {
      "Action": "dms:LoginDatabase",
      "Effect": "Allow",
      "Resource": "acs:rds:*:*:dbinstance/rds783a0639ks5k7328y"
    }
  ],
  "Version": "1"
}
```

请将 `rds783a0639ks5k7328y` 替换为您要授权的 RDS 实例 ID。

授权子用户登录所有 RDS

授权策略样例如下：

```
{
  "Statement": [
    {
      "Action": "dms:LoginDatabase",
      "Effect": "Allow",
      "Resource": "acs:rds:*:*:*"
    }
  ],
  "Version": "1"
}
```

11 RDS授权样例

如果您的租户账号购买了10个RDS实例。而作为RAM管理员，您希望仅仅授权其中的2个RDS实例给某个RAM用户。那么您可以创建如下的授权策略：

说明：

授予该策略的RAM用户是可以列出所有的RDS实例，但只能操作（比如DeleteDBInstance操作）其中的两台。目前，不支持RAM用户仅仅查看自己有访问权限的RDS实例。

```
{
  "Statement": [
    {
      "Action": "rds:*",
      "Effect": "Allow",
      "Resource": [
                  "acs:rds:*:*:dbinstance/i-001",
                  "acs:rds:*:*:dbinstance/i-002"
                  ]
    },
    {
      "Action": "rds:Describe*",
      "Effect": "Allow",
      "Resource": "*"
    }
  ],
  "Version": "1"
}
```

12 负载均衡 SLB 授权

问题

- 查看 SLB 的权限定义
- 为一个子用户授予只读访问 SLB 的权限
- 为一个子用户授予完全管理 SLB 的权限
- 授权一个子用户管理两台指定的 SLB 实例
- 已经授权子用户管理某个负载均衡器的权限，但是在均衡器实例中添加/移除 ECS 服务器以及设置权重时提示没有权限

查看 SLB 的权限定义

请参考 SLB OpenAPI 文档中的 RAM鉴权 部分。

为一个子用户授予只读访问 SLB 的权限

在 RAM 控制台中创建一个子用户，并为此子用户附加系统授权策略“AliyunSLBReadOnlyAccess”。附加授权策略的方式请参考授权。

为一个子用户授予完全管理 SLB 的权限

在 RAM 控制台中为此子用户附加系统授权策略 “AliyunSLBFullAccess”。

授权一个子用户管理两台指定的 SLB 实例

您需要使用自定义授权策略的功能。假设您的两台实例 ID 分别是 i-001 和 i-002。

首先您需要创建一条自定义授权策略，包含管理 i-001、i-002 的权限以及查看 SLB 所有资源的权限：

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "slb:*",
      "Resource": [
                  "acs:slb:*:*:loadbalancer/i-001",
                  "acs:slb:*:*:loadbalancer/i-002"
                  ]
    },
    {
      "Effect": "Allow",
      "Action": "slb:Describe*",
      "Resource": "*"
    }
  ],
  "Version": "1"
```

```
}
```

然后为此用户添加此条自定义授权策略。

已经授权子用户管理某个负载均衡器的权限，但是在均衡器实例中添加/移除 ECS 服务器以及设置权重时提示没有权限

在负载均衡器中关于 ECS 服务器操作的接口，不仅检查 SLB 的资源权限，还要检查 ECS 服务器的权限；避免一个子用户拥有某个负载均衡器的权限后，可以将任意服务器加入此均衡器实例。

例如，如果希望将 i-001 这台 ECS 加入 SLB-001 这个负载均衡器，那么需要授予此账号如下权限：

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "slb:AddBackendServers",
      "Resource": ["acs:slb:*:*:loadbalancer/slb-001"]
    },
    {
      "Effect": "Allow",
      "Action": "slb:AddBackendServers",
      "Resource": ["acs:ecs:*:*:instance/i-001"]
    },
    {
        "Effect": "Allow",
        "Action": "slb:DescribeLoadBalancers",
        "Resource": "acs:slb:*:*:loadbalancer/*"
    }
  ],
  "Version": "1"
}
```

如果您希望简化授权，只要授权一个负载均衡器的管理权，就可以向此实例中添加任意服务器，以及设置任意实例的权重，可以参考下面的授权策略。此授权策略在 ECS 资源上添加了所有 SLB 的操作权限。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "slb:*",
      "Resource": [
                  "acs:slb:*:*:loadbalancer/i-001",
                  "acs:slb:*:*:loadbalancer/i-002"
                  ]
    },
    {
      "Effect": "Allow",
      "Action": "slb:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "slb:*",
      "Resource": "acs:ecs:*:*:*"
```

```
    }
  ],
  "Version": "1"
}
```

13 SLB授权样例

- Use Case #1

  如果您的租户账号购买了10个SLB实例。而作为RAM管理员，您希望仅仅授权其中的2个SLB实例给某个RAM用户。那么您可以创建如下的授权策略：

  说明：

  授予该策略的RAM用户是可以列出所有的SLB实例，但只能操作（比如DeleteLoadBalancer操作）其中的两台。目前，不支持RAM用户仅仅查看自己有访问权限的SLB实例。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "slb:*",
      "Resource": [
                  "acs:slb:*:*:loadbalancer/i-001",
                  "acs:slb:*:*:loadbalancer/i-002"
                  ]
    },
    {
      "Effect": "Allow",
      "Action": "slb:Describe*",
      "Resource": "*"
    }
  ],
  "Version": "1"
}
```

- Use Case #2

  RAM用户将一台后端ECS服务器（如i-001)添加到SLB实例（如slb-001）。具体策略如下：

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "slb:AddBackendServers",
      "Resource": ["acs:slb:*:*:loadbalancer/slb-001"]
    },
    {
      "Effect": "Allow",
      "Action": "slb:AddBackendServers",
      "Resource": "acs:ecs:*:*:instance/i-001"
    }
  ],
  "Version": "1"
}
```

- Use Case #3

RAM用户将您租户账号中的任意后端ECS服务器添加到SLB实例（如slb-001）。具体策略如下：

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "slb:*",
      "Resource": ["acs:slb:*:*:loadbalancer/slb-001"]
    },
    {
      "Effect": "Allow",
      "Action": "slb:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "slb:*",
      "Resource": "acs:ecs:*:*:*"
    }
  ],
  "Version": "1"
}
```

14 内容分发 CDN 授权

问题

授权子用户执行刷新缓存及预热操作

授权子用户执行刷新缓存及预热操作

您可以创建如下授权策略，包含 CDN 只读、刷新缓存及预热权限：

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "cdn:Describe*",
        "cdn:PushObjectCache",
        "cdn:RefreshObjectCaches"
      ],
      "Resource": "acs:cdn:*:*:*",
      "Effect": "Allow"
    }
  ]
}
```

然后将新创建的权限授权给子用户。

15 CDN授权样例

如下的授权策略允许一个RAM用户对CDN资源的READ、Push和Refresh操作。

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "cdn:Describe*",
        "cdn:PushObjectCache",
        "cdn:RefreshObjectCaches"
      ],
      "Resource": "acs:cdn:*:*:*",
      "Effect": "Allow"
    }
  ]
}
```